

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-14. (Cancelled)

15. (Currently Amended) A computer system comprising:

a processor;

a memory coupled to said processor;

at least one nonvolatile data store;

a communication device for communicating over a communications link to an external device; a second computer system;

a port for communicatively coupling said computer system and said communication device over a bus having a plurality of data lines;

at least one bus communicatively coupling said memory, said peripheral controller, and said port to each other, to said at least one data store, and to said processor; and

switch means for controlling a data communications pathway between said communications device and said at least one data store to prevent data received over said communications link and said communications device via said port to prevent access to said at least one data store by viral, hacker, or other malicious computer software code.

~~a switch coupled within said data line selected from said plurality of data lines for enabling and disabling said communication device.~~

16. (Currently Amended) A ~~The~~ computer system of according to claim 15 wherein said communication device is a network interface card disposed within a main computer hardware box of said computer system and said switch means is affixed to~~coupled with~~ said network interface card.

17-18. (Cancelled)

19. (New) A computer system according to claim 15, wherein the external device comprises one of a second computer system, a network, and an Internet.

20. (New) A computer system according to claim 15, wherein:

 said port for communicatively coupling said computer system and said communication device couples said communications device over a bus having a plurality of data lines; and

 said switch means for controlling comprises a switch coupled within a data line selected from said plurality of data lines for enabling and disabling said communication device.

21. (New) A computer system according to claim 15, wherein:

 said at least one nonvolatile data store comprises a first data store and a second data store; and

 said switch means for controlling a data communications pathway between said communications device and said at least one data store comprises a data-store switch for modifying the accessibility of at least one of the first and second data stores according to a access status of said communications device.

22. (New) A computer system comprising:

 a processor;

 a memory coupled to the processor;

 at least one non-volatile data store;

 a data port;

 a communication device for communicating over a communications link to an external device; and

 at least one of a (i) data store switch and (ii) a communications device switch, the data-store switch operative to modify the accessibility of at least one data store according to a access status of said communications device, and the communications device switch operative to modify the accessibility of said communications device by said computer including by said at least one data store according to a access status of said communications device.

23. (New) A computer system according to claim 22, wherein the at least one non-volatile data store comprises first and second data stores and said data-store switch for modifying the accessibility of at least one of the first and second data stores by the computer.

24. (New) A computer system according to claim 23, wherein the data port is operative to mediate and selectively link the computer to other devices over the communications link.

25. (New) A computer system according to claim 24, wherein the computer is operable in: (i) a connected state wherein the computer may use the data port to obtain data from another device over the communications link and the data-store switch may enable the second data store, and in (ii) a disconnected state wherein the computer may not use the data port to obtain data from another device over the communications link and the data-store switch may enable the first data store, so that the computer may enable only one of the first and second data stores at any given time and the data store enabled depending upon whether the computer is accessing the communications link or not accessing the communications link, and data received over the communications link being isolated only to the second data store.

26. (New) A computer system according to claim 25, wherein if the data received over the communications link included a virus, hacking, or other malicious executable code, then the virus, hacking, or other malicious executable code is confined to the second data store.

27. (New) A computer system according to claim 23, wherein the switching of the first and second data stores may be done under manual, hardware or software control;
under manual control, a user controlling the state of the data-store switch; and
under software control, the data store switch responds programmatically to a processor in the computer to control the accessibility of the first and second data store according to the connected or disconnected state of the computer.

28. (New) A computer system according to claim 27, wherein the computer is operable to execute an Internet browser application program, the communications link comprises a communications link to the Internet, and the processor programmatically recognizes the intended or actual launch of the Internet browser and controls the state of the data-store switch to make the second data store the only accessible data store when data is received from the Internet over the communications link.

29. (New) A computer system according to claim 25, wherein operating the data store switch between from the connected state and the disconnected state optionally includes re-booting the computer in order to make the selected one of the first and second data store the only data store available in the selected state.

30. (New) A computer system according to claim 25, wherein only the second data store is available during operation in the connected state.

31. (New) A computer system according to claim 25, wherein only the first data store is available during operation in the disconnected state.

32. (New) A computer system according to claim 25, wherein both the first data store and the second data store are available during operation in the disconnected state.

33. (New) A computer system according to claim 25, wherein an Internet browser application program stored on the second data store launches automatically when the computer boots from the second data store.

34. (New) A computer system according to claim 23, wherein the computer synchronously switches the data port and the second data store so that the first data store is never accessible when the data port is active, thereby improving the resistance of the computer to viral infection and hacking.

35. (New) A computer system according to claim 30, wherein the second data store includes application program software to process the data received over the communications link so that there is no need to migrate the received data from the second data store to the first data store.

36. (New) A computer system according to claim 30, wherein the second data store includes application program software to process the data received over the communications link so that there is no need to migrate the received data from the second data store to the first data store.

37. (New) A computer system according to claim 30, wherein the data received over the communications link and initially stored on the second data store is migrated to the first data store, and the procedure for migrating includes executing an anti-virus software before performing a copy operation between simultaneously enabled first and second data stores.

38. (New) A computer system according to claim 37, wherein the migration includes a predetermined time delay to obtain and execute newly prepared and distributed security software addressing threats that have come to light since the time of receipt of the data over the communications link that is stored on the second data store and the copying of data from the second data store to the first data store.

39. (New) A computer system according to claim 23, wherein the computer further comprises a communications device enabling switch for enabling and disabling access by the computer to the communications device.

40. (New) A computer system according to claim 39, wherein the enabling and disabling access is accomplished by one of powering up or down the communications device and altering a state of a data line on a communications bus coupling the communications device to the computer to alter the ability of the communications device to transfer data to a data port of the computer.

41. (New) A computer system according to claim 40, wherein the communications device operated in conjunction with the communications link is selected from the set of communications devices consisting of an acoustic modem, a POTS telephone line, a tap, an Ethernet, a wireless modem, and radiation-permeable space.

42. (New) A computer system according to claim 25, wherein the connected state comprises a network connected state and the disconnected state comprises a network disconnected state.

43. (New) In a computer system of the type having a processor, a memory coupled to the processor, at least one non-volatile data store, a data port, and a communication device for communicating over a communications link to an external device; a method of operating the computer system to protect the system degradation by from viral, hacker, and other malicious code contamination, the method comprising:

providing at least one of a (i) data store switch and (ii) a communications device switch; and

when the data-store switch is provided, operating the computer system to modify the accessibility of at least one data store according to a access status of said communications device; and

when the communications device switch is provided, operating the computer system to modify the accessibility of said communications device by said computer including by said at least one data store according to a access status of said communications device.

44. (New) A method according to claim 43, wherein:

the at least one non-volatile data store comprises first and second data stores and said data-store switch for modifying the accessibility of at least one of the first and second data stores by the computer;

the data port is operative to mediate and selectively link the computer to other devices over the communications link;

operating the computer in:

(i) a connected state wherein the computer may use the data port to obtain data from another device over the communications link and the data-store switch may enable the second data store, and

(ii) a disconnected state wherein the computer may not use the data port to obtain data from another device over the communications link and the data-store switch may enable the first data store, so that the computer may enable only one of the first and second data stores at any given time and the data store enabled depending upon whether the computer is accessing the communications link or not accessing the communications link, and data received over the communications link being isolated only to the second data store; and

wherein if the data received over the communications link included a virus, hacking, or other malicious executable code, then the virus, hacking, or other malicious executable code is confined to the second data store.